Московский институт электроники и математики имени А. Н. Тихонова

Кафедра информационной безопасности киберфизических систем

Москва 2025

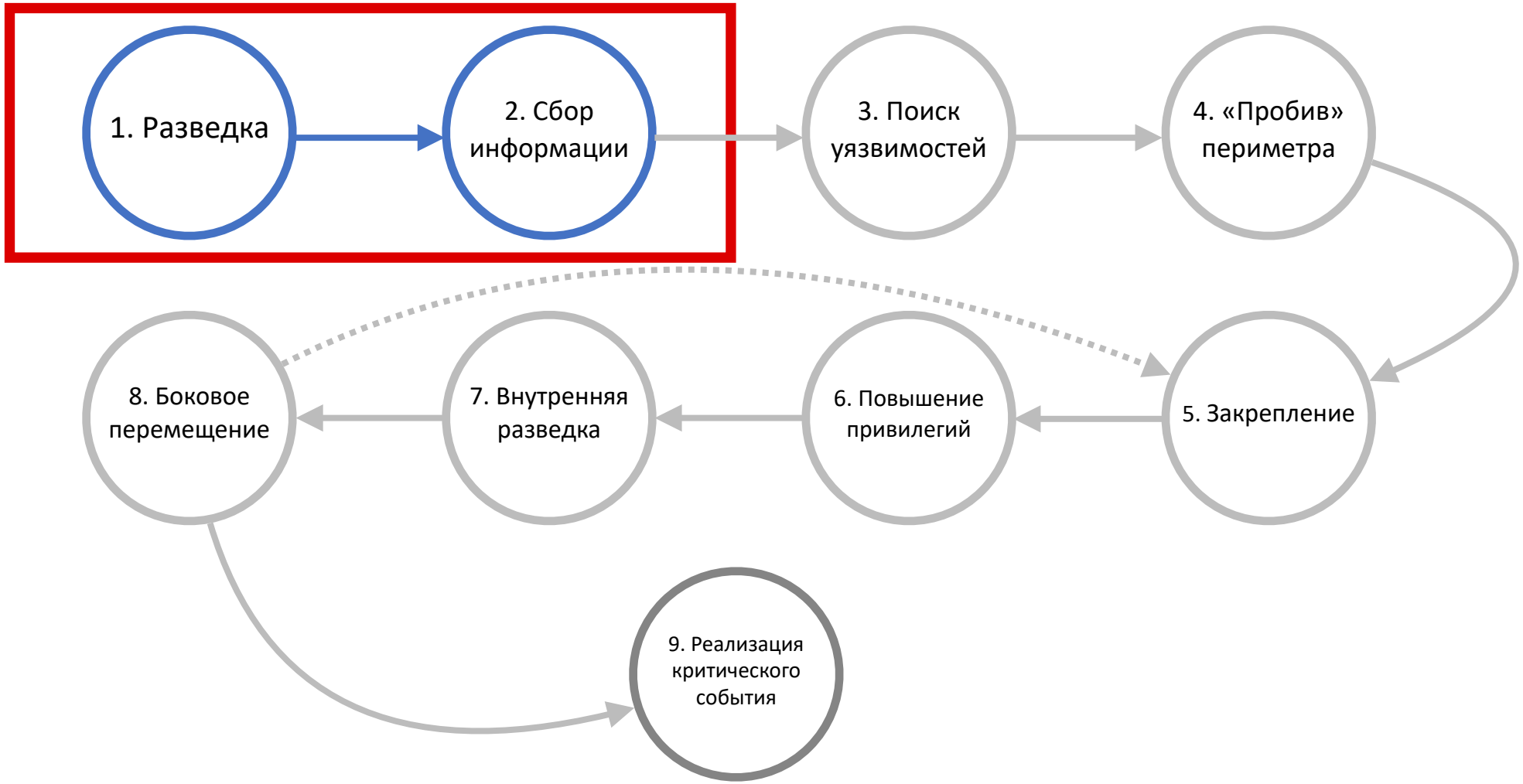
Лекция 2: Разведка и сбор информации о цели

Курс: Технологии пентестинга

Автор: Космачев Алексей Алексеевич

План лекции

1. Поиск TLD(+1)
2. Получение информации от NS
3. Поиск поддоменов
4. Фильтрация
5. Поиск виртуальных хостов
6. Поиск подсетей
7. Поиск сервисов
8. Поиск директорий веб-приложений
9. Определение стека технологий
10. Прочие техники

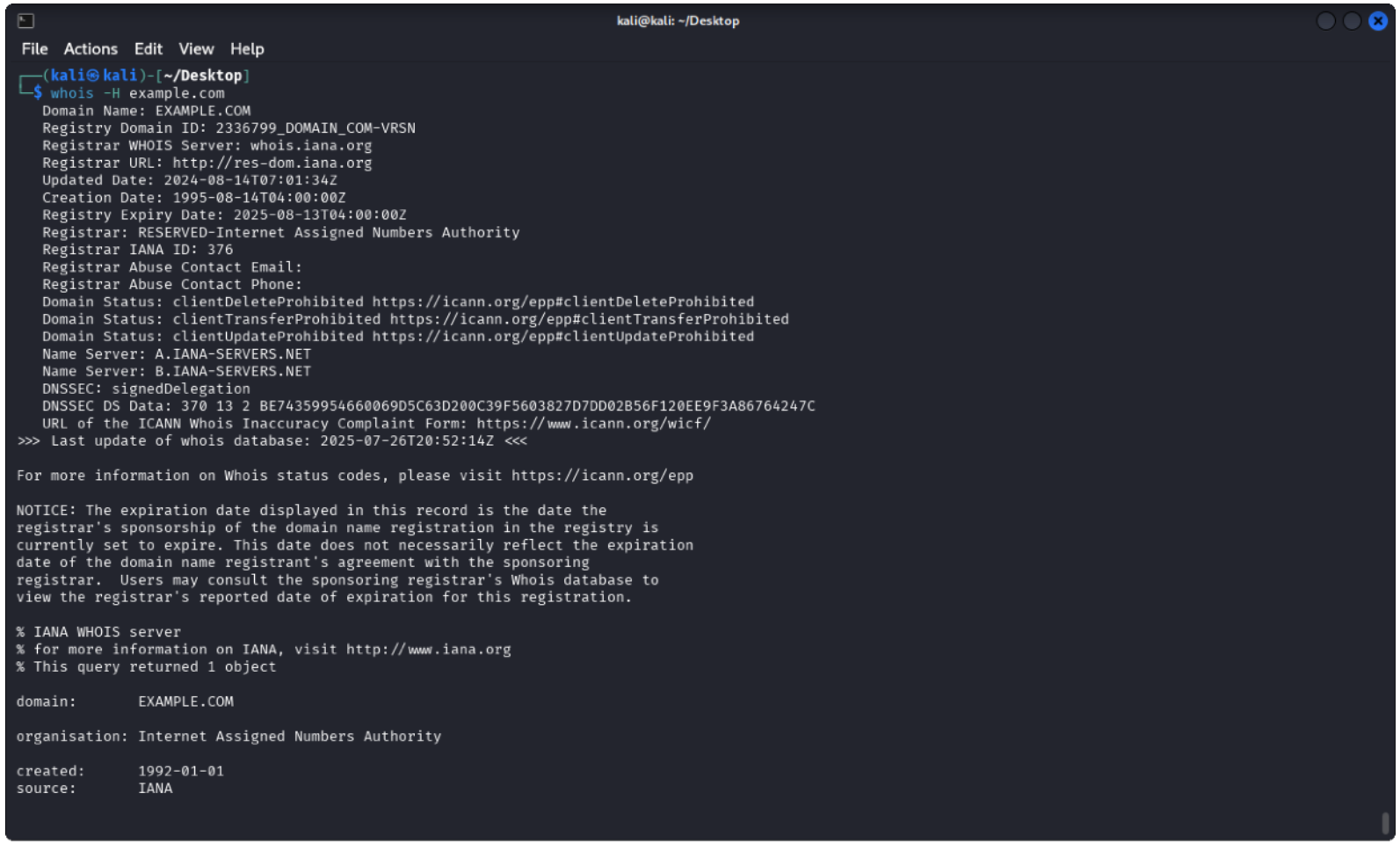

1. Разведка
2. Сбор информации
3. Поиск уязвимостей
4. «Пробив» периметра
5. Закрепление
6. Повышение привилегий
7. Внутренняя разведка
8. Боковое перемещение
9. Реализация критического события

Исходные знания: название компании

Поиск TLD(+1)

Что такое TLD?

Whois


kali@kali: ~/Desktop
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ whois -H example.com
Domain Name: EXAMPLE.COM
Registry Domain ID: 2336799_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.iana.org
Registrar URL: http://res-dom.iana.org
Updated Date: 2024-08-14T07:01:34Z
Creation Date: 1995-08-14T04:00:00Z
Registry Expiry Date: 2025-08-13T04:00:00Z
Registrar: RESERVED-Internet Assigned Numbers Authority
Registrar IANA ID: 376
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: A.IANA-SERVERS.NET
Name Server: B.IANA-SERVERS.NET
DNSSEC: signedDelegation
DNSSEC DS Data: 370 13 2 BE74359954660069D5C63D200C39F5603827D7DD02B56F120EE9F3A86764247C
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-07-26T20:52:14Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object
domain: EXAMPLE.COM
organisation: Internet Assigned Numbers Authority
created: 1992-01-01
source: IANA

Утилиты

- dnsrecon (https://github.com/darkoperator/dnsrecon)
- crobat (https://github.com/Cgboal/SonarSearch)
- amass (https://github.com/owasp-amass/amass)

```
dnsrecon -t tld -d example.com
crobat -t example.com
```

→

```
amass intel -whois -df tld.txt
```

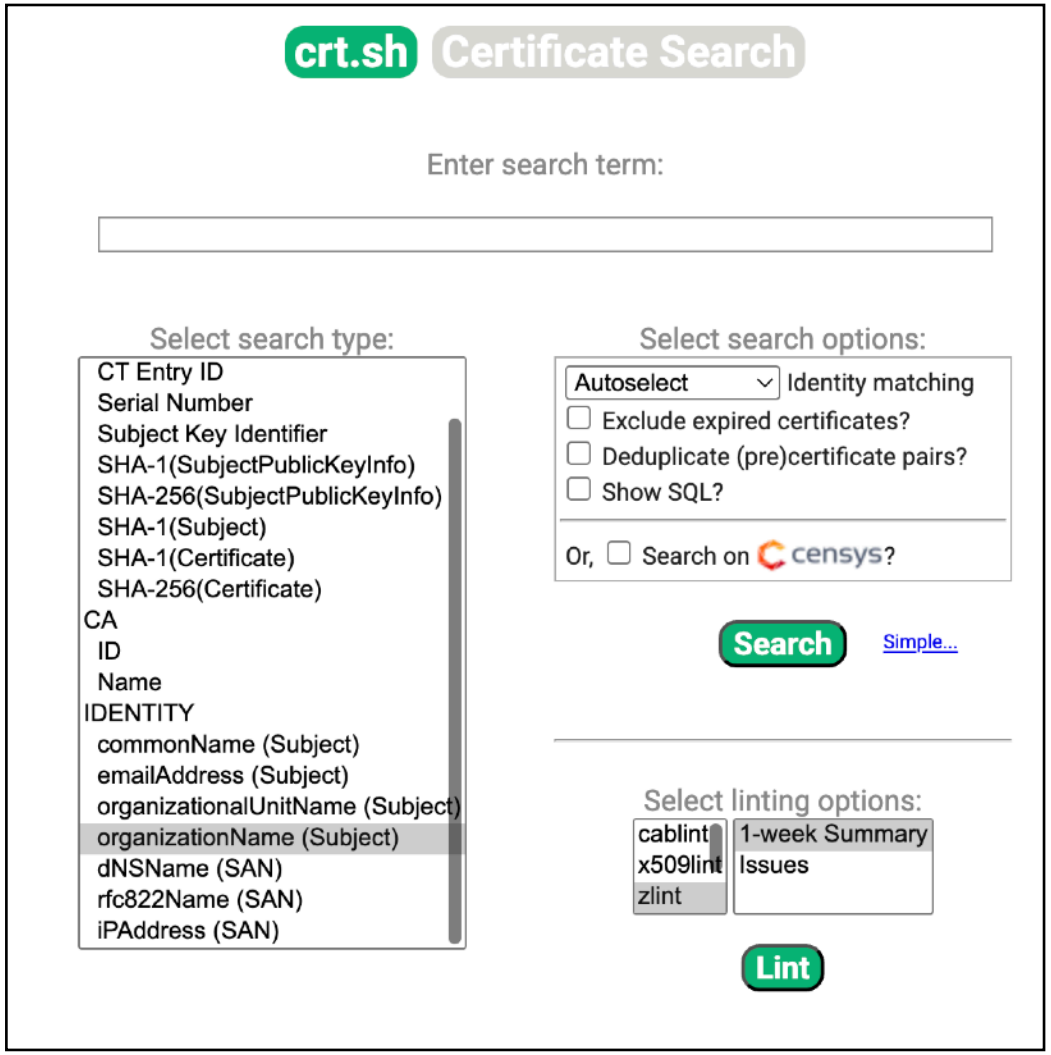
Большой риск Fasle-Positive

SSL (Certificate Transparency)

Certificate Transparency - проект, согласно которому CA обязаны публиковать информацию о каждом выпущенном сертификате

- Делаем поиск по выпущенным SSL-сертификатам компании

```
https://crt.sh/?o=organization+name
https://crt.sh/?q=example.com
https://crt.sh/?a=1
```

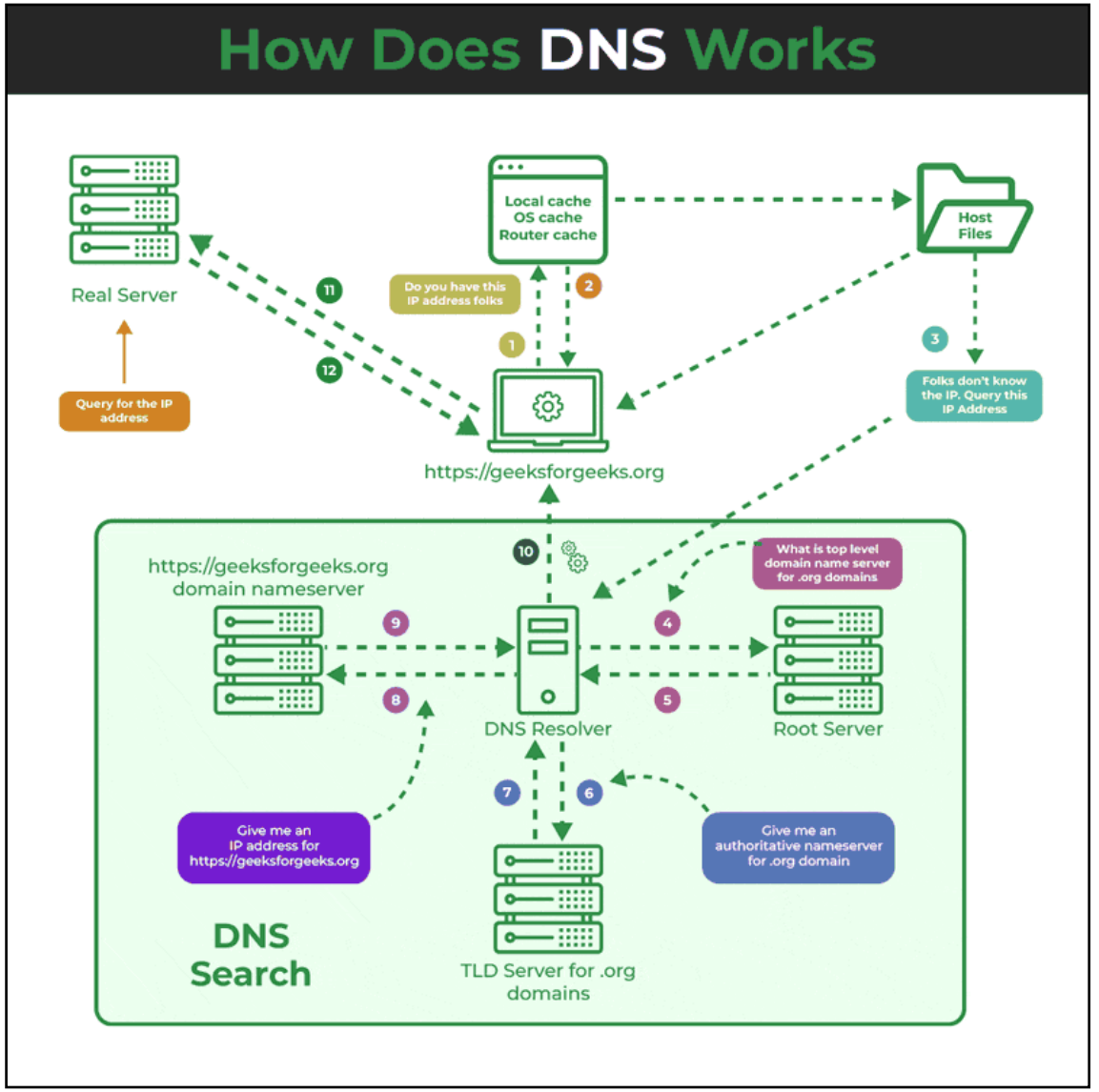


Получение информации от NS

DNS

Основные типы записей:

- A: IPv4 адрес
- AAAA: IPv6 адрес
- CNAME: алиас на другой домен
- MX: доменное имя почтового сервера
- **NS: список серверов, ответственных за разрешение доменных имен (Name Servers)**
- PTR: используется для обратной связи (IP->доменное имя)
- TXT: текстовое поле



Zone Transfer

- Репликация DNS-записей с одного NS-сервера на другой
- Осуществляется при помощи AXFR-запросов
- Если имеется мисконфигурация, выполнить данную операцию может кто угодно
- ВАЖНО! Это крайне шумная и агрессивная операция

```
dig axfr @ns.server.domain target.domain
host -l target.domain ns.server.domain
dnsrecon -a -d "target.domain"
```

Reverse NS Lookup

- Поиск доменов, использующих конкретный NS
- В некоторых случаях позволяет получить список поддоменов

https://viewdns.info/reversens/?ns=ns.server.domain

Поиск поддоменов

Утилиты

- zdns (https://github.com/zmap/zdns)
- altdns (https://github.com/infosec-au/altdns)
- dnsx (https://github.com/infosec-au/altdns)
- shuffledns (https://github.com/projectdiscovery/shuffledns)
- gobuster (https://github.com/OJ/gobuster)
- ffuf (https://github.com/ffuf/ffuf)
- dnsrecon (https://github.com/darkoperator/dnsrecon)
- crobat (https://github.com/Cgboal/SonarSearch)
- amass (https://github.com/owasp-amass/amass)

```
amass enum -passive -df tld.txt -config your.config
amass enum -passive -norecursive -noalts -df tld.txt -config your.config
crobat -s example.com
dnsrecon -d "target.domain"
```

SSL (Certificate Transparency)

- findomain (https://github.com/Findomain/Findomain)
- subfinder (https://github.com/projectdiscovery/subfinder)
- assetfinder (https://github.com/tomnomnom/assetfinder)

```
findomain -t "target.domain" -a
subfinder -d "target.domain"
assetfinder "target.domain"
```

APIs

Можно использовать API следующих сервисов

AlienVault, BinaryEdge, BufferOver, BuiltWith, C99, Censys, Chaos, CIRCL, DNSDB, DNSTable, FacebookCT, GitHub, HackerOne, HackerTarget, NetworksDB, PassiveTotal, RapidDNS, Riddler, SecurityTrails, Shodan, SiteDossier, Spyse, Twitter, Umbrella, URLScan, VirusTotal, WhoisXML, ZETAlytics, Cloudflare

Имеется интеграция данных сервисов с amass с указанием API-ключа

Shodan

- Shodan (https://www.shodan.io/)
- nrich (https://gitlab.com/shodan-public/nrich)

Shodan:

```
hostname:"target.domain"
```

nrich (Shodan cli):

```
echo 127.0.0.1 | nrich -
nrich ip_list.txt
```

В некоторых случаях можно также получить имеющиеся уязвимости

Subdomain brute-forcing

Subdomain brute-forcing

1. Получение списка резолверов (NS-серверов); также, можно использовать собственные NS-сервера компании

```
wget https://raw.githubusercontent.com/wavvs/lazydns/master/resolvers.txt
```

2. Получение списка потенциальных поддоменов

```
https://github.com/assetnote/commonspeak2-wordlists/blob/master/subdomains/subdomains.txt
https://github.com/danielmiessler/SecLists/blob/master/Discovery/DNS/dns-Jhaddix.txt
https://github.com/wavvs/lazydns/blob/master/wordlists/normal.txt
https://github.com/wavvs/lazydns/tree/master/wordlists/big.txt
```

Subdomain brute-forcing

3. Запуск перебора

```
zdns A --name-servers=@resolvers.txt -input-file wordlist.txt -threads 50 -retries 3 -go-processes 5 | tee result_A.json
zdns CNAME --name-servers=@resolvers.txt -input-file wordlist.txt -threads 50 -retries 3 -go-processes 5 | tee result_CNAME.json
zdns AAAA --name-servers=@resolvers.txt -input-file wordlist.txt -threads 50 -retries 3 -go-processes 5 | tee result_AAAA.json
```

4. Поиск измененных доменных имен для обнаруженных доменов

```
altdns -i resolved_domains.txt -w words.txt -o permutated.txt
```

Subdomain brute-forcing

5. Разрешение (Resolve) доменных имен

```
zdns A --name-servers=@resolvers.txt -input-file permutated.txt -threads 50 -retries 3 -go-processes 5 | tee result_A.json
zdns CNAME --name-servers=@resolvers.txt -input-file permutated.txt -threads 50 -retries 3 -go-processes 5 | tee result_CNAME.json
zdns AAAA --name-servers=@resolvers.txt -input-file permutated.txt -threads 50 -retries 3 -go-processes 5 | tee result_AAAA.json
```

Дополнительные утилиты:

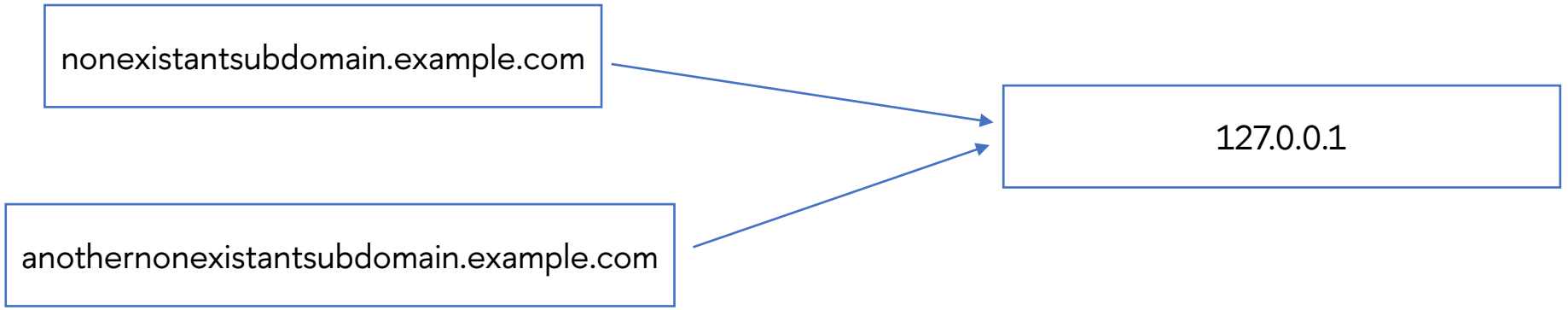
```
dnsrecon -t brt -d "target.domain" -n "nameserver.com" -D "/path/to/wordlist"
gobuster dns --domain "target.domain" --resolver "nameserver" --wordlist "/path/to/wordlist"
```

Фильтрация

Wildcard domains

- DNS-запись вида:

```
*.example.com A 127.0.0.1
```



Быстрая проверка на Wildcard domains

```
dig a 'nonexistentdomain0123456789.example.com'
dig a ‘*.example.com'
```

Замечания:

- В некоторых конфигурациях разрешен wildcard-домен, однако не будет ответа на запрос *.example.com
- В некоторых конфигурациях будет имитироваться wildcard-домен, однако разный контент будет отображаться при обращении по разным поддоменам (виртуальные хосты)

Проверка на Wildcard domains

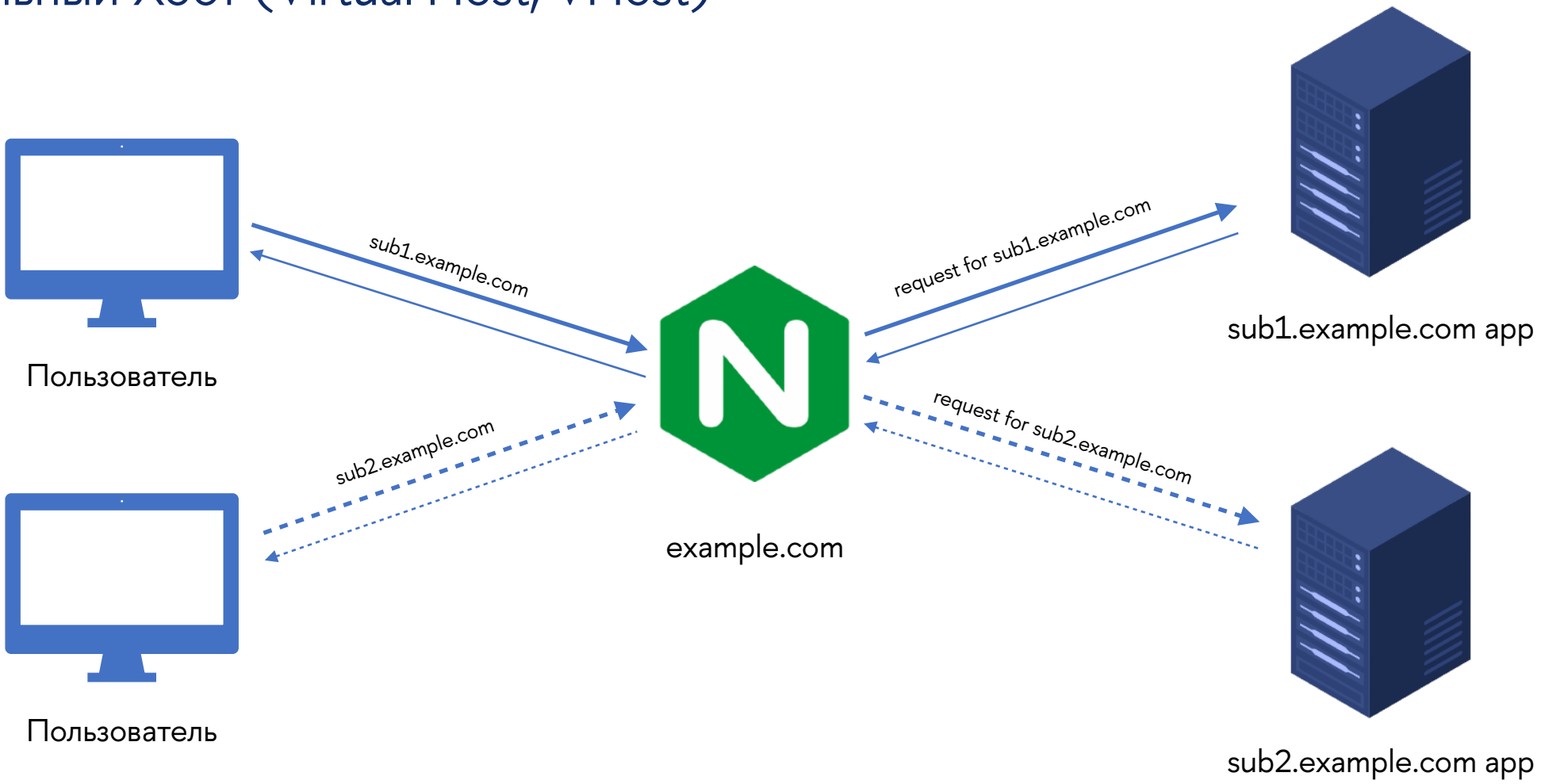
```
dnsx -r resolvers.txt -l wordlist.txt -wd domain.to.filter.com -o output.txt
shuffledns -d domain.to.filter.com -list wordlist.txt -r resolvers.txt
```

Утилиты считают количество доменов, которые разрешаются в один и тот же IP-адрес

При преодолении лимита домены будут проверяться на wildcard

Поиск виртуальных хостов

Виртуальный Хост (Virtual Host, VHost)



Утилиты

- Burp Suite Intruder (https://portswigger.net/burp)
- ffuf (https://github.com/ffuf/ffuf)
- wfuzz (https://github.com/xmendez/wfuzz)
- gobuster (https://github.com/OJ/gobuster)

```
gobuster vhost --wordlist "/path/to/wordlist.txt" --url your_url
wfuzz -H "Host: FUZZ.target.domain" --hc 404,403 -c -z file,"/path/to/wordlist.txt" your_url
ffuf -w /path/to/wordlist.txt -u https://target.domain -H "Host: FUZZ"
ffuf -H "Host: FUZZ.target.domain" -c -w "/path/to/wordlist.txt" -u your_url
ffuf -c -r -w "/path/to/wordlist.txt" -u «http://FUZZ.target.domain/"
```

Поиск подсетей

Онлайн-поиск

```
https://securitytrails.com/domain/target.domain/history/a
https://viewdns.info/iphistory/?domain=target.domain
```

PTR-записи

```
dnsrecon -r 127.0.0.1/24 -d .
amass intel -ip -src -addr 127.0.0.1
amass intel -ip -src -cidr 127.0.0.1/24
amass intel -ip -src -asn 2025
```

Базы данных Forward DNS (FDNS)

```
crobat -r 127.0.0.1/24
amass intel -addr 127.0.0.1
amass intel -cidr 127.0.0.1/24
amass intel -asn 2025
```

Поиск сервисов

Утилиты

- nmap (https://nmap.org/) - медленнее, но точнее
- masscan (https://github.com/robertdavidgraham/masscan) - быстрее, но менее точный

```
nmap -Pn -p- --open -vv -T4 -iL subdomains.txt -oA nmap_results
nmap -Pn -sV -p- --open -vv -iL subdomains.txt -oA nmap_results
nmap -Pn -sV -p- --open -vv --version-all -iL subdomains.txt -oA nmap_results
```

Поиск веб-приложений

- httpx (https://github.com/projectdiscovery/httpx)
- httprobe (https://github.com/tomnomnom/httprobe)

```
httpx -ports 80,81,443,2053,2078,2079,2080,2083,2087,2090,2091,2096,2435,2942,5021,5353,5656,5357,5985,6092,6767,7080,7081,7088,7183,7419,7706,8008,8080,8081,8088,8172,8181,8401,8443,8880,8888,9001,9002,9003,9004,9419,9525,9998,15672,33034,47001,47279,52223,52227,52229,52231,52233 -l subdomains.txt > http_subdomains.txt
```

Визуальное отображение веб-приложений

- aquatone (https://github.com/michenriksen/aquatone)
- WitnessMe (https://github.com/byt3bl33d3r/WitnessMe)
- EyeWitness (https://github.com/RedSiege/EyeWitness)

```
cat http_subdomains.txt | aquatone
cat nmap.xml | aquatone -nmap
```

Поиск директорий веб-приложений

Поиск по источникам

- gau (https://github.com/lc/gau)
- waybackurls (https://github.com/tomnomnom/waybackurls)

```
cat domains.txt | waybackurls > urls.txt
cat domains.txt | gau -b ttf,woff,svg,png,jpg > urls.txt
```

Фаззинг (Fuzzing)

- gobuster (https://github.com/OJ/gobuster)
- ffuf (https://github.com/ffuf/ffuf) - может делать рекурсивный фаззинг
- dirsearch (https://github.com/maurosoria/dirsearch) - может делать рекурсивный фаззинг
- dirb (http://dirb.sourceforge.net/)
- dirbuster (https://sourceforge.net/projects/dirbuster/)
- wfuzz (https://github.com/xmendez/wfuzz)
- feroxbuster (https://github.com/epi052/feroxbuster) - может делать рекурсивный фаззинг

```
ffuf -w /path/to/wordlist -u https://target.domain/FUZZ
ffuf -c -w "/path/to/wordlist.txt" -maxtime-job 60 -recursion -recursion-depth 2 -u your_url/FUZZ
gobuster dir --wordlist "/path/to/wordlist.txt" --url your_url
wfuzz --hc 404,403 -c -z file,"/path/to/wordlist.txt" your_url/FUZZ
feroxbuster -w "/path/to/wordlist.txt" -u http://target.domain/
```

Фаззинг (Fuzzing)

Важно!

Фаззинг часто может вызывать отказ в обслуживании (DoS) из-за большого количества запросов в секунду (особенно ffuf и feroxbuster), поэтому скорость работы утилит нужно ограничивать

Fuzzing Wordlists

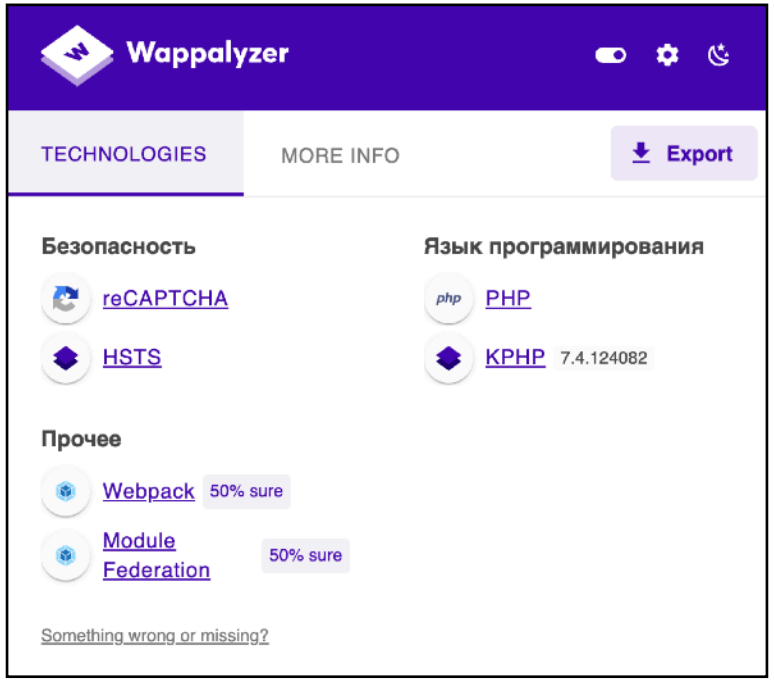
- https://github.com/Bo0oM/fuzz.txt/blob/master/fuzz.txt
- https://wordlists.assetnote.io
- https://github.com/assetnote/wordlists
- **https://github.com/danielmiessler/SecLists/tree/master/Discovery/Web-Content**
- https://github.com/random-robbie/bruteforce-lists

Определение стека технологий

Утилиты

- whatweb (https://github.com/urbanadventurer/whatweb)
- wappalyzer (https://www.wappalyzer.com/)

```
whatweb https://terget.domain
```



Определение языка программирования по расширению файла в URL

- .php, .php5, phtml, ... -> PHP
- .aspx -> C#/VB.NET (ASP.NET)
- .asp -> VBScript (classic ASP)
- .jsp, .jspx, .do -> Java
- .pl -> Perl
- .py -> Python (встречается редко)
- .rb -> Ruby (встречается редко)

https://target.domain/profile.php

Прочие техники

Google Dorks

- «» - поиск конкретного вхождения
- -test - исключение страниц, содержащих «test»
- site:example.com - поиск только по доменам «site.com»
- inurl:keyword - поиск по ключевым словам в URL
- filetype:xls - поиск по расширениям файлов
- И много другого...

https://gist.github.com/sundowndev/283efaddbcf896ab405488330d1bbc06

https://www.exploit-db.com/google-hacking-database (Примеры)

Существуют подобные для других браузеров и Git

`site:*.target.domain -www` ← Поиск поддоменов, исключая уже найденные (www)

Cloud discovery

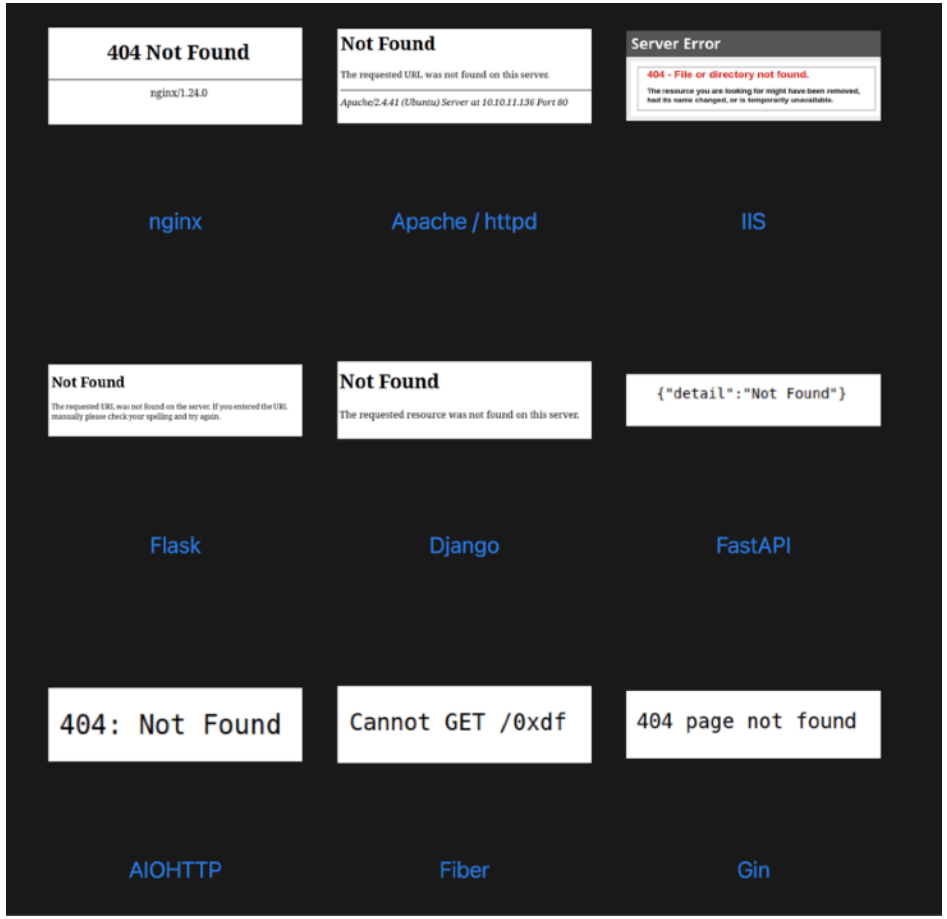
- s3recon (https://github.com/clarketm/s3recon)
- grayhatwarware (https://buckets.grayhatwarfare.com/)

```
s3recon "keywords-list.txt" -o "results.json" --public
https://buckets.grayhatwarfare.com/buckets/0/BUCKET_NAME
https://buckets.grayhatwarfare.com/results/FILE_NAME
```

На что еще обращаем внимание

- Информация на странице (Секции Credits, Contacts)
- Нестандартные HTTP-заголовки
- Файлы robots.txt, sitemap.xml, .DS_Store, ...
- Комментарии и метаданные (HTML-, CSS-, JS-файлы)
- Логи ошибок (StackTrace)

Бонус: определение веб-сервера по стандартной ошибке 404



https://0xdf.gitlab.io/cheatsheets/404

@LEXA_MALOSPAAL

@HUN7_0R_B3_HUN73D


ВЫСШАЯ • ШКОЛА • ЭКОНОМИКИ •